基于超奇异同源的零知识证明及群签名方案 *

赵兴波，李梦东†，王　颖，朱屹霖

(北京电子科技学院 密码科学与技术系，北京 100070)

摘　要： Bullens 等人在 CSI-Fish 中留下一个开放问题，即设计一个识别协议，允许系统挑战空间是 $\mathbb{Z}_N$，而不是小集合 $\{-S,\cdots,S\}$。本文提出了一个基于超奇异同源的零知识证明方案。该方案将挑战 C 作为一个同源，从而解决了这一问题，并实现了更小的稳固性误差以及公钥长度。该方案也可以通过 Fiat-Shamir 变换为非交互零知识证明，进而可以在量子随机预言下实现基于超奇异同源的签名方案以及群签名方案。且本文分析了方案的安全性以及正确性。

关键词： 零知识证明；超奇异；同源；群签名

中图分类号： TP　　doi: 10.19734/j.issn.1001-3695.2021.12.0705

Zero-knowledge proof and group signatures based on supersingular isogeny

Zhao Xingbo, Li Mengdong†, Wang Ying, Zhu Yilin

(*Dept. of Cryptology Science & Technology*, *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*)

Abstract: Bullens et al. left an open problems in CSI-Fish is to devise a identification protocol that allows for the challenge set to be $\mathbb{Z}_N$ rather than the small set $\{-S,\cdots,S\}$. This paper proposed a zero-knowledge proof scheme based on supersingular isogeny. This scheme addresses the open problem by taking the challenge C as a isogeny , and reduces the soundness error and the size of public key. This scheme can be turned into non-interactive zero-knowledge proof scheme using the Fiat-Shamir transform. Then signature scheme and group signature scheme based on supersingular isogeny can be implemented under the quantum random oracles model. And this paper analyzes the security and correctness of these schemes.

Key words: zero-knowledge proof; supersingular; isogeny; group signature

0　引言

同源密码是后量子密码学的一个很有发展前景和研究价值的候选者。同源是两条椭圆曲线之间保持基点的同态映射，是一种群同态[1]。基于同源的密码系统在开始主要研究通常曲线[2,3]，但因为通常曲线同源问题存在亚指数时间的量子算法，而 Biasse 等人[4]研究发现超奇异同源问题的量子算法为指数时间，因此目前同源密码大多是超奇异椭圆曲线上的方案。

目前构造同源签名的基础主要是以下两个同源问题：计算超奇异同源(CSSI)问题[5]和类群作用逆问题(GAIP)[6]。且基于同源的签名大多是结合 Fiat-Shamir 变换来构造的[7,8]。在[9,10]中提出的基于 CSSI 的签名方案,即使在最优化的变体[10]中也产生至少 12KB 大小的签名。另一方面，依靠 GAIP 并采用 Fiat-Shamir with aborts 方法, De Feo 和 Galbraith 提出了一个新的签名方案，称为 SeaSign[11]。SeaSign 提供的签名非常小，在 128 位安全级别下小于 1 千字节。最近, Beullens[12] 等人通过计算理想类群，改进了 SeaSign 并获得了第一个实用的基于同源的签名方案，命名为 CSI-FiSh。它允许从理想类群中进行均匀抽样，并对其元素进行规范表示。CSI-FiSh 只需要 390 毫秒来签名或验证消息，签名大小只有 263 字节。因此，基于 CSI-FiSh 同源特征的签名是非常实用的。

通过对 CSI-FiSh 方案以及其他基于超奇异同源签名方案的研究与分析，本文提出了一种基于超奇异同源的零知识证明系统。该系统改进了 Bullens 等人提出的 CSI-Fish 中的证明系统，解决了 CSI-Fish 中提出的开放问题，即将系统的挑战空间由小集合 $\{-S+1,S-1\}$ 提升为 CSIDH-512 中理想类群的阶数 N。本方案与 CSI-FiSh 方案相比具有更小的稳固性误差以及公钥长度，本文仅需一个椭圆曲线作为公钥。基于该证明系统，本文构造了基于超奇异椭圆曲线同源的签名方案以及群签名方案，并对签名方案的进行了安全性证明。

1　背景知识

1.1　超奇异椭圆曲线及同源

椭圆曲线之间的同源 $\varphi: E\to E_1$ 为一个态射，也是群同态且 $\varphi(\mathcal{O}_E)=\mathcal{O}_{E_1}$。Tate 指出[13]:有限域 $\mathbb{F}_p$ 上的两条椭圆曲线 E, E_1 是同源的当且仅当 $\#E(\mathbb{F}_q)=\#E_1(\mathbb{F}_q)$。

对于同源 $\varphi: E\to E_1$，当 E=E_1 时称为自同态。椭圆曲线的自同态集用 End(E) 表示，具有点加法和函数复合运算的环结构[14]。在 $\mathrm{End}_p(E)$ 中，E 的 Frobenius 自同态 π 满足特征方程: $\pi^2-t\pi+q=0$，t 称为 Frobenius 迹。当且仅当 t=0 时，曲线 E 是超奇异的。Fp-有理自同态环 $\mathrm{End}_p(E)$ 是虚二次域 K=$\mathbb{Q}$ $k=\mathbb{Z}(\sqrt{-p})$ 的序 $\mathcal{O}$。$\mathrm{End}_p(E)$ 中总是包含 $\mathbb{Z}[\pi_q]$ 这个子环。

设 $\mathcal{E}\ell\ell(\mathcal{O},\pi)$ 表示在 $\mathbb{F}_p$ 上定义的所有超奇异椭圆曲线 E 的集合，设 $\mathcal{O}$ 是虚二次域的序 $\pi\in\mathcal{O}$ 使得 $\mathcal{E}\ell\ell(\mathcal{O},\pi)$ 非空。理想类群 cl($\mathcal{O}$) 自由地和传递地作用于集合 $\mathcal{E}\ell\ell(\mathcal{O},\pi)$，在 $\mathcal{O}$ 和 $\mathrm{End}_p(E)$ 之间存在一个 Frobenius 映射使得 $\varphi(\mathcal{O}_E)=\mathcal{O}_E$ 且 $(x,y)\to(x^p,y^p)$，用⋆表示这一作用[15]。最近，该作用⋆被用来设计几种密码原语—CSIDH 及其延伸签名方案 SeaSign、CSI-Fish 等。这几种方案的安全性都是基于类群作用逆问题，定义如下:

问题 1(类群作用逆问题—Group Action Inverse Problem: GAIP)给定两个曲线 E_0，E_1，其自同态环 $End(E_0)$=$End(E_1)=\mathcal{O}$, 找到一个理想 $\mathfrak{a}\subset\mathcal{O}$ 使得 $E_1=\mathfrak{a}\star E$。

1.2　CSI-Fish

Beullens 等人提出了一种基于 CSIDH-512 困难性的有效

收稿日期： 2021-12-19；**修回日期：** 2022-04-01　**基金项目：** 教育部信息安全一流专业建设点项目

作者简介： 赵兴波(1996-)，男，辽宁凌源人，硕士研究生，主要研究方向为密码学；李梦东(1964-)，男(通信作者)，山东利津人，教授，主要研究方向为密码算法及其应用(lmd@best.edu.cn)；王颖(1998-)，女，北京怀柔人，硕士研究生，主要研究方向为密码学；朱屹霖(1998-)，女，河南新乡人，硕士研究生，主要研究方向为密码学.

签名方案。对于在 CSIDH 中为 CSIDH-512 参数集选择的素数集 $l_1 \cdots l_{74}$，Beullens 等人确定了自同态环的相关类群是循环的，由 g 生成，且阶数 N=cl($\mathcal{O}$) 由下式给出

$$N=3\times37\times140718\times51593604295295\\867744293584889\times31599414504681\\995853008278745587322049 09$$

对于任何理想 $\mathfrak{a}\in$ cl($\mathcal{O}$)，可以写作 $\mathfrak{a}=g^a$，其中 $a\in\mathbb{Z}_N$，因为群是循环的。只要使用 CSIDH-512 参数集，任何人都可以对类群元素进行均匀采样，并拥有唯一的表示。对于与 E_0 同源的椭圆曲线 E'，简化符号 $\mathfrak{a}\star E_0=[a]E_0$ 有了这个符号，就有了 $[a]([b]E_0)=[a+b]E_0$[12]。

1.3 零知识证明

零知识证明(zero-knowledge proof：ZKP)是证明者和验证者之间的双方协议，证明者通过和验证者交互，向验证者证明它知道一些秘密信息，而除了声明本身已经揭示的之外，不透露任何关于秘密的信息。

对于一个语言 $L\subseteq\{0,1\}^*$，其中的串 x 都伴随着一个二元关系 R$\subseteq\{0,1\}^*\times\{0,1\}^*$，存在 w 使得 $(x,w)\in$R，w 称为 x$\in L$ 的证据(witness)。参考[16]，下面对零知识证明进行定义：

定义 1 设 (P,V) 是一个双方协议，其中 V 是概率多项式时间(probabilistic polynomial time:PPT)算法，设 L，$L'\subseteq\{0,1\}^*$ 是具有二元关系 R，R' 的语言，使得 $R\subseteq R'$ 当且仅当它满足下列条件， 那么 (P,V) 称为 L，L' 具有完全性误差 α，挑战集 C，公共输入 x 和秘密输入 w 的 Σ 协议。

三轮形式(Three-move form)：协议的形式如下:证明者 P 在输入 (x,w) 时，计算承诺 t 并将其发送给验证者 V。验证者 V 在输入 x 时，选择一个挑战 $c\leftarrow C$ 并将其发送给 P。证明者向验证者发送一个响应 r。根据协议文本 (t,c,r)，验证者最终接受或拒绝证明。

证明系统需要具有以下三个性质：

完全性(Completeness):对于一个诚实的证明者 P 和验证者 V，当任一 $(x,w)\in$R，则验证者接受的概率至少为 1-α。

特殊稳固性(Specia Soundness)：存在一种 PPT 算法 K(知识提取器)，其将满足 $c\neq c'$ 的两个接受文本 (t,c,r)，(t,c',r') 作为输入，并输出 w'，使得 $(x,w')\in R'$。稳固性误差 δ=1/C。

诚实验证者零知识(Honest-Verifier Zero Knowledge: HVZK)：存在以 x$\in L$ 和 c$\in C$ 为输入的 PPT 模拟器，该算法输出 (t,r)，使得三元组 (t,c,r) 与由真实协议运行生成的协议文本不可区分[16]。

一个 3 轮-特殊稳固的-诚实验证者零知识证明协议，可以应用 Fiat-Shamir 转换将其转换为非交互式零知识证明协议。

定义 2 一个规范的认证方案 ID=(K, P, V, c),其中 K 是概率多项式时间的密钥生成算法,在输入安全参数 λ 时输出一对 (pk,sk)；P 也是 PPT 算法，输入 sk 输出一条消息 m；c ≥ 1 是挑战的整数位长度；V 是一种确定性多项式时间验证算法，将 pk 和证明文本作为输入，输出 0 或 1[17]。

1.4 签名

一个签名方案 S = (KeyGen,Sign,Verify) 由如下三个算法组成:

- **KeyGen** (1^λ) ：密钥生成算法输入安全参数 λ，输出一对公/私钥对 (pk,sk)。
- **Sign** (sk,m)：签名算法输入私钥 sk 和消息 m，输出一个签名 σ。
- **Verify** (pk,m,s)： 验证算法输入公钥 pk，消息 m 和签名 σ，输出一个比特，1 代表 σ 是消息 m 的一个合法签名，0 代表不合法。

定义 3 选择消息攻击下的不可伪造性：EUF-CMA 安全,如果对于所有 PPT 敌手 A，有 $\mathrm{Adv}_{A,S}^{EUF\text{-}CMA}(1^\lambda)$=Pr[A win] = negl (1^λ) 则一个签名方案 S 是 EUF-CMA 安全的[18]。

定理 1[10] 设 R 与生成算法 K 是困难关系，令 (P,V) 是 Σ 协议中 R 的证明者和验证者，对于某些整数 c≥1 具有 c 比特挑战。假设 Σ 协议是完整的，特殊稳固的以及诚实验证者零知识的。那么 (K, P, V, c) 是一个规范的识别方案，在被动攻击下是安全的。

定理 2[10] 令 ID 是一个规范的认证方案，在被动攻击下是安全的。设 S 为使用 Fiat-Shamir 变换从 ID 中导出的签名方案。在随机预言模型下，S 在选择消息攻击下是不可伪造的。

1.5 群签名

下面介绍群签名的定义以及安全模型。

定义 4 群签名。群签名方案由下面的五个多项式时间算法组成:

- **GSetup**：输入安全参数，生成系统公共参数和群公，私钥对 (GM_{pk},GM_{sk})；
- **GJion**：成员加入是由用户和群管理员执行的交互式算法，若算法成功，则用户成为有效的群成员，并得到公、私钥对 (U_{pk},U_{sk})；
- **GSign**：对于给定的消息 m，其签名由管理员和群成员共同合作完成;
- **GVerify**：验证者根据群公钥和消息 m 对签名进行验证;
- **GTrace**：通过该算法，管理员 GM 可以找出对消息 m 真正的签名者。

群签名的安全性定义需满足以下性质:

1) 正确性：对于给定的消息 m，只有经合法的群成员运行签名算法产生的群签名才能够被正确的验证。

2) 不可伪造性：只有合法的群成员通过和管理员交互才能够产生被验证正确的群签名。

3) 匿名性：只有群管理员能够确定签名者的身份，其他人只能验证群签名是否正确。

4) 可跟踪性：当出现矛盾争端的时候，管理员可以通过追踪算法打开群签名，识别出具体的签名者身份，并给出证据。

5) 抗合谋性：即使多个群成员合谋在一起，也不能产生有效的被管理员追踪不到的群签名。

2 新的零知识证明以及签名方案

2.1 零知识证明的身份认证协议

对于 CSIDH-512 参数集，CSI-FiSh 指出其理想类群是循环的，具有已知阶数 N 和生成元 $\mathfrak{g}$。只要使用 CSIDH-512 参数集，任何人都可以对类群元素进行均匀采样，并拥有唯一的表示。在此基础上，本文描述了新的基于超奇异同源问题的身份认证协议(如图 1)，与 CSI-Fish 中的身份认证协议相比，本文的认证协议实现了更小的稳固性误差(soundness error)，且具有更小的公钥长度。

零知识证明协议的设置如下：

参数设置：选取大素数 $p=4\cdot l_1\cdots l_n-1$，其中 l_i 是小的不同的奇素数，给定集合 $\mathcal{E}\ell\ell(\mathcal{O},\pi)$ 和理想类群以及在 $\mathbb{F}_p$ 上具有自同态环的超奇异椭圆曲线 E_0，为了证明秘密 a 的知识，证明者与验证者进行如下 Σ 协议操作，如图 2。

密钥生成：选取一个随机的同源 $[a]:E_0\rightarrow E_1$，得到一个随机椭圆曲线 E_1。公钥为 E_1，密钥为 a。

识别协议如下:

承诺：证明者随机选取 $b\in_R\mathbb{Z}_N$，且 $b\neq a$，将 $E=[b]E_0$ 发送给验证者。

挑战：验证者检验 E 是否等于 E_1，若相等，则拒绝。否则随机选取挑战 $c\in\mathbb{Z}_N$，然后发送给证明者。

响应：证明者发送 $r=c+b-a \bmod N$ 给验证者。

验证：验证者检查是否 $[r]E_1=[c]E=E_2$，相等则接受；否

则拒绝。

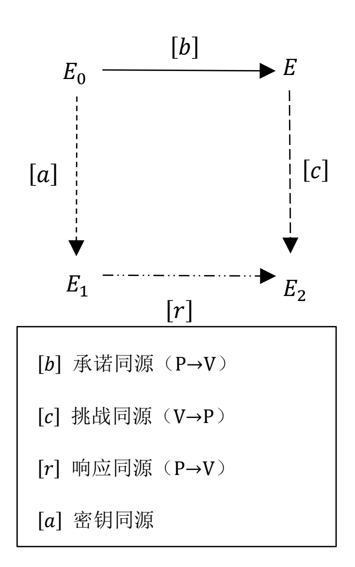


图 1　识别协议

Fig. 1　Identification protocol

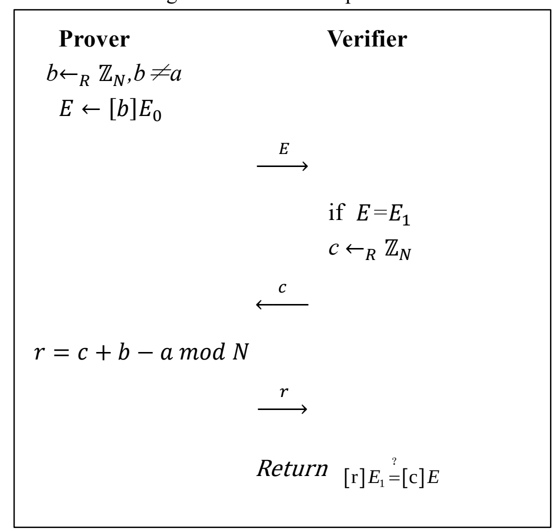


图 2　零知识证明

Fig. 2　Zero knowledge proof

2.2　安全性分析

定理 3　基于同源的识别协议是一个完整和安全的 Σ 协议，它具有完全性、特殊稳固性以及诚实验证者零知识的。

证明:　**完全性**：假设证明者的行为总是诚实的，即其知道一个秘密 $E_1=[a]E_0$。验证者检查 $[r]E_1=[c]E=E_2$ 是否成立,因为 $[r]E_1=[c][b][a]\ E_1=[c][b][a][-a]E_0=[c][b]E_0=[c]E$ 这证明了验证者总是接受诚实生成的证明。

特殊稳固性：给定两个具有不同挑战的有效证明，即 $\pi=(E,c,r)$ 和 $\pi'=(E,c',r')$，其中 $c\neq c'$　那么 $r\neq r'$。本文有 $[r]E_1=[c]E$ 以及 $[r']E_1=[c']E$，因此可以提取 $(c-c')+(r-r')$，其为 GAIP 问题的一个解。与此同时，作弊证明者不能通过验证，除非它成功猜测挑战 c。特别是，由于挑战空间现在是 $\mathbb{Z}_N$，其中包含 N 个元素，所以该协议实现了 1/N 的稳固性误差。

诚实验证者零知识：为了模拟证明，从 $\mathbb{Z}_N$ 中随机抽取样本 c，模拟器从 $\mathbb{Z}_N$ 中随机抽取 r。计算 $E_2=[r]E_1$ 并输出证明 $\pi=(E,c,r)$。根据决策 GAIP 问题，模拟器生成的证明与诚实执行的挑战等于 c 的协议证明是无法区分的，因为真实证明和模拟证明都具有 r 以及 $E_2=[r]E_1$ 的均匀随机分布值作为响应，因此该认证协议诚实验证者零知识的。

2.3　签名方案

在算法 1 到算法 3 中描述了基于同源的签名方案，该方案的安全性基于 GAIP 困难假设。它是通过对 2.1 节中介绍的零知识证明协议应用 Fiat-Shamir 变换得到的。其主要思想是用临时密钥 E 以及消息 m 的哈希值来替换挑战 c，即 $c=H(E\|m)$。签名 σ 由 r, E 组成，验证者计算 $c'=H(E\|m)$，并检查是否 $[r]E_1=[c']E$。为了减少了签名的大小，

下面详细描述了基于超奇异同源的签名方案，具体如下：

算法 1　**KeyGen**

输入：初始曲线 E_0　以及理想类群的阶数 N

输出：公、私钥对 (sk, pk) .

$a \leftarrow_R \mathbb{Z}_N$

$E_1=[a]E_0$

$pk=E_1$

return $(sk=a, pk=E_1)$

算法 2　**Sign**

输入：消息 m 以及私钥 sk

输出：签名 $\sigma=(r,E)$.

$b \leftarrow_R \mathbb{Z}_N, b\neq a$

$E=[b]E_0$

$c=H(E\|m)$

$r=c+b-a \bmod N$

return　$\sigma=(r,E)$

算法 3　**Verify**

输入：消息 m, E_0 ,公钥 pk 以及签名 σ

输出：Valid 或 Invalid.

$(r,E)\leftarrow\sigma$

$c'=H(E\|m)$

If　$[r]E_1=[c']E$ then

1. ***return***　Valid
2. Else
3. ***return***　Invalid

2.4　安全性分析

定理 4　在随机预言模型中，上述基于超奇异同源的签名方案具有选择消息攻击下的不可伪造性，即 EUF-CMA 安全。

证明:　如上一节所示，该身份认证方案(Σ 协议)具有特殊稳固性和诚实验证者零知识。因此，定理 1 意味该认证方案是安全的，可以抵御假冒被动攻击。由定理 2 可知，该签名方案在随机预言模型中是 EUF-CMA 安全的。

2.5　对比分析

CSI-Fish 中描述的基础身份认证协议如下:证明者为了证明其知道一个群元素ɑ使得 $E_1=[a]E_0$，然后证明者随机选取 $b\in\mathbb{Z}_N$，并将 $E=[b]E_0$ 发送给验证者。验证者随机选取比特 c∈$\{0,1\}$，然后发送给证明者。当 c=0 时，证明者回复 r=b，验证者检查是否 $E=[r]E_0$；当 c=1 时，证明者回复 $r=b-a \bmod N$，验证者检查 E 是否等于 $[r]E_1$。该协议的挑战空间仅为二进制比特 c∈ $\{0,1\}$，公钥长度为 1 个曲线。

为了降低稳固性误差,CSI-Fish 增加了挑战空间，但这也增加了公钥的大小。其方法为选择一个正整数 S，密钥是 S-1 维的向量，如 $(a_1,\cdots,a_{S-1})$，公钥为 $(E_0,[a_1]E_0,\cdots,[a_{S-1}]E_0)$。证明者现在必须证明它知道一个秘密 $s\in\mathbb{Z}_N$，使得 $E_j=[s]E_i$ 出现在公钥列表中的某对椭圆曲线上。证明者再次随机选择 $b\in\mathbb{Z}_N$，并通过 $E=[b]E_0$ 来对它进行承诺。验证者从集合 $\{-S+1,S-1\}$ 中均匀地采样挑战 c，证明者用 $r=b-a_c \bmod N$ 来响应。验证检查 $E=[r]E_c$，当 c 为负值时，有 $E_{-c}=E_c^t$。CSI-FiSh 的这种适应方案实现了 $1/2S-1$ 的安全稳固性，公钥长度为 S-1 个曲线。

在 CSI-FiSh 的基础上，证明者可以简单地模仿基于离散对数的构造，因为现在可以在环 $\mathbb{Z}_N$ 中工作，因此可以创建特有的响应，来表达临时密钥、秘密密钥和挑战的组合。然而，主要的问题是验证者如何验证这个组合是正确的，因为当考虑曲线 $g^a\star E$ 时，群作用只允许在 g 的指数上增加一个已知

的常数。也就是，若像在经典 DH 中进行系数乘($r=b+ac$)的形式，则群作用就成为了映射 $g^a \to (g^a)^c$，但在环 $\mathbb{Z}_N$ 的环境下是不存在这种类似映射的[18]。

本文方案将挑战 c 视作一个同源，这样做的好处是可以将临时密钥 b 和挑战 c 结合到一起，变为[b+c]的形式,避免出现 $g^a \to (g^a)^c$ 的情况。且这样做使得挑战 c 可以在环 $\mathbb{Z}_N$ 中随机选取，也就使得挑战空间变为类群阶数 N，从而实现了 1/N 的安全稳固性。但是采用这种方案的缺点是需要多计算一次同源，即 $E_2=[c]E$，这增加了计算时间，提高了额外计算量。本文的方案公钥长度为 1 个椭圆曲线。表 1、表 2 分别给出了本文方案与 CSI-Fish 中的识别协议与签名方案的比较结果。

表 1　识别协议方案比较

Tab. 1　Comparison of Identification protocol

方案	公钥长度	挑战空间	稳固性误差	同源次数
CSI-Fish 基础方案	1	{0,1}	1/2	2
CSI-Fish 适应方案	S-1	{-S+1,S-1}	1/2S-1	2

表 2　签名方案比较

Tab. 2　Comparison of Signature scheme

方案	公钥长度	签名长度	同源次数
CSI-Fish 签名方案	S	2S	2S
本文签名方案	1	2	2

3　基于新 ZK 的群签名方案

在群签名中，为了代表群签名，群成员需要生成一个 NIZK 来证明他有一个有效的密钥/公钥对。签名包括密文和证明(消息嵌入在证明中)。为了验证签名，验证者只是检查证明的有效性。下面，本文给出了本文的群签名方案的详细描述。它与[19] 一样借助状态列表的方法实现群签名,[19]中采用双线性映射来实现成员的身份认证，但本文采用上面提出的同源 ZK 来实现。用同源来实现群签名方案的优点是密钥短、抗量子攻击等，但缺点是计算量更大，计算时间较长。

本群签名方案存在公钥状态列表 L_{PK}、群管理员 GM、群成员 U_i 以及可信时间戳机构 4 类实体。其中，公钥状态列表中显示当前群成员的身份信息 ID_i、公钥 E_i、授权签名起始时间 $Time_{start}$ 和终止时间 Time_{end}；管理员 GM 负责群成员的加入、群签名的追踪以及实时更新维护，并向所有群成员广播最新的 L_{PK}；可信时间戳机构负责向群管理员及群成员提供时间戳服务；群成员 $\mathrm{U_i}$ 负责完成群签名。

3.1　基于超奇异同源的群签名方案

本文方案包含系统建立、成员加入、签名、验证和追踪五个步骤。

1) 系统建立

选取大素数 $p=4\cdot l_1\cdots l_n-1$，其中 l_i 是小的不同的奇素数，给定集合 $\mathcal{E}\ell\ell(\mathcal{O},\pi)$ 和理想类群以及在 $\mathbb{F}_p$ 上具有自同态环的超奇异椭圆曲线 E_0，$H_1:\{0,1\}^*\to\mathbb{Z}_N$，$H_2:\{0,1\}^*\to\mathbb{Z}_N$。对于 GM:取 $x\leftarrow_R\mathbb{Z}_N$，计算 $E_{GM}=[x]E_0$，其中 x 为群管理员私钥，E_{GM} 为公钥。故群公共参数为 $\{p,N,E_0,H_1,H_2\}$，群公钥为 E_{GM}。

2) 成员加入

成员 U_i 想要加入，先随机选取 $x_i,a_i\leftarrow_R\mathbb{Z}_N$，计算 $E_i=[x_i]E_0$，$h_i=a_i+H_1(ID_i)\bmod N$，$E_{IDi}=[a_i]E_0$，最后将 (ID_i,E_{IDi},E_i,h_i) 发送给 GM。其中 ID_i 代表成员 U_i 的现实身份信息。

收到 (ID_i,E_{IDi},E_i,h_i) 后，GM 先验证等式 $[H_1(ID_i)]E_{IDi}=[h_i]E_0$ 是否成立，确认 ID_i 的有效性。若成立，计算 $E_{GMi}=[x]E_i$，将 E_{GMi} 发送给 U_i，并存储 ID_i、E_i。其中 ID_i、E_i 以及时戳 Time 构成公开的公钥状态列表 L_{PK} 见表 3。

成员 U_i 收到 E_{GMi} 后，计算 $E_{GMi}=[x_i]E_{GM}$ 是否成立。若成立，则成员 U_i 公钥为 E_i，私钥为 x_i。

3) 群签名过程

群成员 U_i 对消息 m 进行签名，需要和管理员 GM 共同完成。

群成员 U_i 随机选择 $b_i\leftarrow_R\mathbb{Z}_N$，并向可信时间戳机构请求当前时间 Time，然后计算 $E_{bi}=[b_i]E_0$，$t_i=H_2(E_i\|E_0\|E_{bi}\|m)$，$s_i=t_i+b_i-x_i \bmod N$，群成员 U_i 将 $(\mathrm{Time},E_i,m,E_{bi},s_i)$ 发送给 GM。

表 3　公钥列表 L_{Pk}

Tab. 3　Public Key list l_{pk}

序号	群成员	成员公钥	开始时间	终止时间
i	ID_i	E_i	$Time_{start-i}$	$\mathrm{Time}_{end\text{-}i}$
⋮	⋮	⋮	⋮	⋮

注：公钥状态列表 L_{PK} 的实时维护由群管理员 GM 负责，每当群成员加入或撤销,都要实时更新 L_{PK}，并向所有群成员广播最新的 L_{PK}，同时将 $(ID_i,E_i,Time_{start-i},Time_{end-i})$ 发送给群成员 U_i，作为群成员 U_i 的群签名证书。设计一个公钥状态列表 L_{PK} 可以实现动态地增加和撤销群成员，提高执行效率。在撤销某个群成员时，只需将 L_{PK} 中群成员对应的终止时间修改为当时的时间即可。当成员被撤销后，它不可以生成新的合法群签名。当群成员公钥有效时，可以将其终止时间设置为一个足够大的值。

GM 接收到 (E_i,m,E_{bi},s_i) 后，先根据 E_i 值查找 L_{PK}，看其在当前时间是否为有效值;若有效,则检验 $t_i'=H_2(E_i\|E_0\|E_{bi}\|m)$，且 $[t_i']E_{bi}=[s_i]E_i$ 是否成立。若成立,则管理员 GM 计算 $E_{vi}=[x+t']E_0$。并将 $ID_{Tra}=(ID_i,m,E_{vi},t_i',s_i)$ 存储到追踪列表，如表 4。群成员对消息 m 的签名记为 $\sigma_i=(E_{vi},t_i',s_i)$。

表 4　追踪列表 L_{Track}

Tab. 4　Track list l_{track}

序号	群成员	ID_{Tra}
i	ID_i	$ID_{Tra}=(ID_i,m,E_{vi},t_i',s_i)$
⋮	⋮	⋮

4) 验证

验证者接收到签名后，检验 $E_{vi}=[t_i']E_{GM}$ 是否成立。若成立，则接受 $\sigma_i=(E_{vi},t_i',s_i)$ 为消息 m 的群签名；否则，不接受。

5) 追踪

关于签名 $\sigma_i=(E_{vi},t_i',s_i)$ 产生矛盾分歧时，群管理员可以通过查询追踪列表中对应的 t_i',s_i 追踪到该签名的签名人 U_i 的身份，GM 根据签名追踪列表中的 $ID_{Tra}=(ID_i,m,E_{vi},t_i',s_i)$ 信息，查找相应 ID_i 证明该签名确实是群成员 U_i 产生的。

3.2　正确性分析

该方案中的系统建立存在管理员与成员双向验证身份的过程。

1)成员加入过程中管理员与成员互验身份。

管理员 GM 接收到成员 U_i 送的 (ID_i,E_{IDi},E_i,h_i) 后，检验 $[H_1(ID_i)]E_{IDi}=[H_1(ID_i)][a_i]E_0=[h_i]E_0$ 成立，则证明了 ID_i 的有效性。管理员完成对成员的检验后，计算 $E_{GMi}=[x]E_i$ 并将其发送给 U_i，U_i 验证 $E_{GMi}=[x_i]E_{GM}$ 是否成立，确认 GM 的身份。

2)签名过程中验证成员身份。

群管理员 GM 和群中成员 U_i 协作生成群签名。在 GM 接收到 $(\mathrm{Time},E_i,m,E_{bi},s_i)$ 后，先首先检验 U_i 在当前时间内是否存在，若成立，则检验 $t_i'=H_2(E_i\|E_0\|E_{bi}\|m)$，且 $[t_i']E_{bi}=[s_i]E_i$ 是否成立，若成立，则证明发送方确为群中成员 U_i。

3)签名的正确性。

验证签名中 E_{vi} 的有效性，即检验 $E_{vi}=[x+t_i']E_0=[t_i']E_{GM}$ 证明群管理员参与了签名过程。

验证 $t_i'=H_2(E_i\|E_0\|E_{bi}\|m)$ 的正确性，即验证:

$$t_i'=H_2(E_i\|E_0\|E_{bi}\|m)=H_2(E_i\|E_0\|[b_i]E_0\|m)$$
$$=H_2(E_i\|E_0\|[s_i+x_i-t_i]E_0\|m)$$

仅需验证 $[b_i]E_0=[s_i+x_i-t_i \bmod N]E_0$。

因为 $s_i=t_i+b_i-x_i \bmod N$，所以 $[b_i]E_0=[s_i+x_i-t_i \bmod N]E_0=$

$[s_i - t_i \bmod N]E_i = [s_i - t_i' \bmod N]E_i$

通过以上分析，证明了本文所提方案的正确性。

3.3 安全性分析

定理 5 匿名性.对于任意多项式时间敌手 A，本方案在随机预言模型下是匿名的。

证明：通过挑战者 C 和敌手 A 之间的游戏完成证明。

G_0 游戏如下：

1) 挑战者 C 输入安全参数 $p=4\cdot l_1 \cdots l_n - 1$，其中 l_i 是小的不同的奇素数，给定集合 $\mathcal{E}\ell\ell(\mathcal{O},\pi)$ 和理想类群 $cl(\mathcal{O})$ 以及在 $\mathbb{F}_p$ 上具有自同态环的超奇异椭圆曲线 E_0，$H_1:\{0,1\}^* \to \mathbb{Z}_N$，$H_2:\{0,1\}^* \to \mathbb{Z}_N$。随机选取 $x \leftarrow_R \mathbb{Z}_N$，计算 $E_{GM} = [x]E_0$。公开群公共参数为 $\{p,N,E_0,H_1,H_2\}$ 以及群公钥 E_{GM}，保留私钥 x。

2) 敌手 A 输入需签名的消息 m，两个群成员 $U_{i_0}, U_{i_1} \in L_{pk}$ 给挑战者 C，挑战者 C 选取 b = 0，其中 $b \in \{0,1\}$，生成群成员 U_{i_b} 对应的私钥 $x_{i_0} \in_R \mathbb{Z}_N$，令实际群成员 $U_i = U_{i_0}$ 执行签名算法。

3) 挑战者 C 运行签名算法,生成签名 $\sigma_i = (E_{vi}, t_i', s_i)$，并发送给敌手 A。

4) 敌手 A 收到签名后给出关于 b 的猜测。

G_1 游戏如下：

G_1 游戏与 G_0 游戏的过程类似，其区别在于挑战者 C 选取 b = 1，其中 $b \in \{0,1\}$，生成群成员 U_{i_b} 对应的私钥 $x_{i_b} \in_R \mathbb{Z}_N$，并用群成员 U_{i_1} 对应的私钥执行签名算法，生成签名 $\sigma_i^* = (E_{vi}^*, t_i^{*\prime}, s_i^*)$，并发送给敌手 A。敌手 A 收到签名后给出关于 b 的猜测。

下面说明假设敌手 A 赢得匿名性攻击游戏的优势 $Adv_A^{anon} = |\Pr[b^* = b] - 1/2| = \varepsilon$ 是可忽略的，只需要证明挑战者 C 用成员 U_{i_b} 的私钥计算生成的群签名 $\sigma_i = (E_{vi}, t_i', s_i)$ 与用群成员 $U_{i_{1-b}}$ 的私钥计算生成的群签名 $\sigma_i^* = (E_{vi}^*, t_i^{*\prime}, s_i^*)$ 是不可区分的即可。

对于签名 σ_i，由签名过程易知，当挑战者 C 用成员 U_{i_b} 的私钥计算签名时，均匀抽样 $b_i \leftarrow_R \mathbb{Z}_N$，$t_i = H_2(E_i \| E_0 \| E_{bi} \| m)$，$s_i = t_i + b_i - x_i \bmod N$，最终生成签名 $\sigma_i = (E_{vi}, t_i', s_i)$；当挑战者 C 用成员 $U_{i_{1-b}}$ 的私钥计算签名时，均匀抽样 $b_i^* \leftarrow_R \mathbb{Z}_N$，并最终生成签名 $\sigma_i^* = (E_{vi}^*, t_i^{*\prime}, s_i^*)$。根据决策 CSIDH，签名 $\sigma_i = (E_{vi}, t_i', s_i)$ 与 $\sigma_i^* = (E_{vi}^*, t_i^{*\prime}, s_i^*)$ 是不可区分的。因此，敌手 A 的优势是 Adv_A^{anon} 可以忽略的。

综上所述，本文提出的基于超奇异同源的群签名满足随机预言模型下的匿名性。

定理 6 不可伪造性。如果 GAIP 问题是困难的，本文提出的基于超奇异同源的群签名在随机预言模型下是不可伪造的。

证明：通过挑战者 C 和敌手 A 之间的游戏完成证明。假设敌手 A 能够以不可忽略的概率 ε 成功伪造签名，下面将展示挑战者 C 如何利用敌手 A 的伪造结果找到一个理想𝔢,构造一个 GAIP 问题的解。敌手 A 与挑战者 C 之间的游戏如下：

1) Setup：输入安全参数，挑战者 C 进行如下操作：

挑战者 C 输入安全参数 $p=4\cdot l_1 \cdots l_n - 1$，其中 l_i 是小的不同的奇素数，集合 $\mathcal{E}\ell\ell(\mathcal{O},\pi)$ 和理想类群以及在 $\mathbb{F}_p$ 上具有自同态环的超奇异椭圆曲线 E_0，$H_1:\{0,1\}^* \to \mathbb{Z}_N$，$H_2:\{0,1\}^* \to \mathbb{Z}_N$。将群公共参数 $\{p,N,E_0,H_1,H_2\}$ 发送给敌手 A。

2)Query：敌手 A 可以进行多项式次访问预言机并进行如下询问，挑战者 C 作出响应，挑战者 C 分别建立列表 L_1, L_2, L_3, L_4 来存储敌手 A 的 H_1 询问、H_2 询问、私钥询问及签名询问，所有列表初始化为空。设在进行私钥及签名询问之前，已进行过所有相关的 Hash 询问。

1) 哈希询问

H_1 询问:A 可以选择群成员身份 ID_i 进行询问,C 检查列表 L_1，若 A 进过此询问，则返回相同结果。否则令 $h_i = a_i + H_1(ID_i) \bmod N$，将 h_i 返回给 A，并将 (ID_i, h_i, a_i) 加入列表 L_1。

H_2 询问：接收到 A 查询输入 (m, E_{bi}) 时，C 检查列表 L_2，若 A 进过此询问，则返回相同结果。否则 C 随机选择 $t_i \leftarrow_R \mathbb{Z}_N$ 返回给 A,，并将 (m, E_{bi}, t_i) 加入列表 L_2。

2) 私钥询问

A 可以选择群成员身份 ID_i 进行私钥询问，C 随机选取私钥 $x_i \leftarrow_R \mathbb{Z}_N$，并输出 $(Upk_i, Usk_i) = (E_i, x_i)$，将私钥返回给 A，并将 (ID_i, E_i, x_i) 加入列表 L_3。

3) 签名询问

A 可以选择群成员身份 ID_i，提交待签消息 m 的签名询问，C 查询列表 L_2，L_3 找到对应记录并用签名算法计算对消息 m 的签名结果 σ_i，随机选取 $b_i \leftarrow_R \mathbb{Z}_N$，计算 $t_i = H_2(E_i \| E_0 \| E_{bi} \| m)$，$s_i = t_i + b_i - x_i \bmod N$，最终生成签名签名 $\sigma_i = (E_{vi}, t_i', s_i)$。

Forgery：敌手 A 向挑战者 C 提交一个消息 m^*，群成员身份为 ID_i^* 以及伪造的群签名 $\sigma_i^* = (E_{vi}^*, t_i^{*\prime}, s_i^*)$ 且满足以下两个条件：敌手 A 没有询问过用户 ID_i^* 的签名私钥；敌手 A 没有询问过 $(E_{vi}^*, t_i^{*\prime}, s_i^*)$ 的签名。

如果签名 $\sigma_i^* = (E_{vi}^*, t_i^{*\prime}, s_i^*)$ 是合法签名，下面将展示挑战者 C 如何利用敌手 A 的伪造结果求得理想𝔢，其为 GAIP 问题的一个解。挑战者 C 查询敌手 A 的询问列表 L_2，若不存在集合 (m^*, E_{bi}^*, t_i^*)，挑战者 C 放弃并终止游戏。否则，因为 $\sigma_i^* = (E_{vi}^*, t_i^{*\prime}, s_i^*)$ 是合法签名，由签名的验证过程，本文有

$$\begin{cases} E_{vi} = [t_i']E_{GM} \\ E_{vi}^* = [t_i^{*\prime}]E_{GM} \end{cases}$$

若 $t_i - t_i^* = 0$，则挑战者放弃游戏，否则可以计算出 $E_{vi} = [t_i - t_i^* \bmod N]E_{vi}^*$。令 $e = t_i - t_i^* \bmod N$，则有 $E_{vi} = [e]E_{vi}^* = \mathfrak{e}\, E_{vi}^*$。即理想𝔢是 GAIP 问题的一个解。

综上所述，如果 GAIP 问题是困难的，本方案在随机预言模型下是不可伪造的。

定理 7 抗合谋性。对于任意多项式时间敌手 A，本方案在随机预言模型下是抗合谋的。

证明：抗合谋攻击是指即使部分成员联合起来也无法产生 GM 追踪不到的合法群签名。在本方案的群成员加入算法中，管理员 GM 将成员身份信息存储在群成员列表中，签名时先通过搜索列表中的存储信息验证成员的身份合法性，验证成功才提供签名帮助，与群成员合作产生签名,避免了群中成员合谋产生无法追踪的签名。此外基于 GAIP 问题的困难性，使群管理员 GM 无法获知群成员的私钥，且群成员之间无法得出其他成员的私钥。最后，群中所有成员以及管理员 GM 的私钥都完全保密，且互相无关。所以，该方案具有抗合谋性。

定理 8 可追踪性。对于任意多项式时间敌手 A，本方案在随机预言模型下是可追踪的。

证明：方案的可追踪性是指管理员可以通过打开签名来找到签名者的真实身份。本方案的签名由管理员和群成员共同完成，在执行签名算法时，用户会先声称自己的部分签名，然后将其发送给 GM，GM 收到签名后，查询用户 U_i 是否在群成员列表中，并通过判断 $[t_i']E_{bi} = [s_i]E_i$ 是否成立来验证用户签名的合法性。在通过验证之后，管理员才会计算签名。同时将其存储到追踪列表里。因此可以看出，管理员 GM 只需通过搜索追踪列表来打开签名，即可查出签名者身份。

此外，攻击者无法在没有群管理员的情况下独自生成合法签名。假设敌手 A 具有增加和撤销群成员的权力以及获得群私钥和群中任意成员的私钥的能力。此外，A 还可以运行签名预言机和打开预言机。

若在 ID_i 下对于消息 M，A 伪造群成员 i 的签名 σ_i，但只要群管理 GM 是安全的，GM 的私钥不被获取，那么 A 就无法伪造出不能被 GM 追踪到的签名。因为群签名是由群成员和群管理员共同合作完成的。U_i 只有在 GM 协助下才可以产

生有效的群签名，而 GM 在协助 U_i 时，将 U_i 的相关身份信息记录在追踪列表 L_{Track} 中，此外因为 GAIP 问题是困难的，是计算不可行的，那么即使群成员被攻破，只要 GM 的私钥未被泄露，签名仍然不可伪造，所以本方案满足可跟踪性。

3.4 性能分析

将本文群签名方案与文献[19]的方案进行比较。[19]中的方案采用双线性映射，实现群管理员对群成员的身份认证，而本文采用的方案为本文第三节中提出的基于同源的零知识身份认证。且同样具有以下优点:

1) 工作效率高:本文提出的签名方案中群签名长度是固定不变的，不随群中成员个数的变化而变化，且签名长度短。公钥和签名长度均与群成员的数量 n 无关，所以整体群签名效率较高。本文方案适合大群组的群签名方案。

2) 动态性: 本文方案设置了公钥状态列表，可以实现动态地增加和撤销群成员，其加入、撤销代价较小，群成员可以随机的加入和撤销。群成员的撤销简单快捷，只要修改群成员对应的终止时间便能实现群成员的即时撤销。

不同之处在于:

1) 本文群签名方案基于同源的 GAIP 问题，由公钥求出私钥是困难的，规避了被撤销成员联合得出其他成员私钥的风险。

2) 本文群签名中群成员的私钥由自己随机选择生成，因此可以抵挡群管理员的陷害攻击。

3) 本文群签名方案包含了超奇异同源的特殊性质，如密钥短、抗量子攻击等，但计算时间长。

4 结束语

本文在 Bullens 等人提出的 CSI-Fish 的基础上，提出了一个新的零知识证明方案。与 CSI-Fish 中的方案相比,该方案在仅有一个公钥的前提下,将挑战空间提升为类群阶数 N,实现了更强的稳固性。同时本文通过应用 Fiat-Shamir 变换，在量子随机预言模型下得到了基于超奇异同源的签名方案以及群签名方案，并对提出的签名方案进行了安全性证明。

参考文献：

[1] Silverman J H. The arithmetic of elliptic curves [M]. Springer Science & Business Media, 2009.

[2] Rostovtsev A, Stolbunov A. Public-key cryptosystem based on isogenies [J]. Cryptology ePrint Archive, 2006/145.

[3] Childs A, Jao D, Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time [J]. Journal of Mathematical Cryptology, 2014, 8 (1): 1-29.

[4] Biasse J F, Jao D, Sankar A. A quantum algorithm for computing isogenies between supersingular elliptic curves [C]// International Conference on Cryptology in India. Springer, Cham, 2014: 428-442.

[5] Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies [C]// International Workshop on Post-Quantum Cryptography. Springer, Berlin, Heidelberg, 2011: 19-34.

[6] Castryck W, Lange T, Martindale C, *et al.* CSIDH: an efficient post-quantum commutative group action [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2018: 395-427.

[7] Fiat A, Shamir A. How to prove yourself: Practicalsolutions to identification and signature problems [C]// Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1986: 186-194.

[8] Abdalla M, An J H, Bellare M, *et al.* From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security [C]// International Conference on the Theory andApplications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2002: 418-433.

[9] Yoo Y, Azarderakhsh R, Jalali A, *et al.* A post-quantum digital signature scheme based on supersingular isogenies [C]// International Conference on FinancialCryptography and Data Security. Springer, Cham, 2017: 163-181.

[10] Galbraith S D, Petit C, Silva J. Identification protocols and signature schemes based on supersingular isogeny problems [C]// International conference on the theory and application of cryptology and informationsecurity. Springer, Cham, 2017: 3-33.

[11] De Feo L, Galbraith S D. SeaSign: Compact isogeny signatures from class group actions [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2019: 759-789.

[12] Beullens W, Kleinjung T, Vercauteren F. CSI-FiSh: Efficient isogeny based signatures through class group computations [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2019: 227-247.

[13] Galbraith S D. Mathematics of public key cryptography [M]. Cambridge University Press, 2012.

[14] DeFeo L. Mathematics of isogeny based cryptography [J]. arXiv preprint arXiv: 1711. 04062, 2017, 12.

[15] Cozzo D, Smart N P. Sashimi: Cutting up CSI-FiShsecret keys to produce an actively secure distributedsigning protocol [C]// International Conference on Post-Quantum Cryptography. Springer, Cham, 2020: 169-186.

[16] Benhamouda F, Camenisch J, Krenn S, *et al.* Betterzero-knowledge proofs for lattice encryption and their application to group signatures [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2014: 551-572.

[17] Bellare M, Poettering B, Stebila D. From identification to signatures, tightly: a framework and generic transforms [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2016: 435-464.

[18] EI Kaafarani A, Katsumata S, Pintore F. Lossy CSI-FiSh: Efficient signature scheme with tight reduction to decisional CSIDH-512 [C]// IACR International Conference on Public-Key Cryptography. Springer, Cham, 2020: 157-186.

[19] Yu Xuan, Hou Shuhui. Efficient and Secure Group Signature Scheme [J]. Communications Technology, 2018, 51 (2): 413-418. 于璇，侯书会. 一种高效安全的群签名方案 [J]. 通信技术, 2018, 51 (2): 413-418.